AMENDMENTS TO THE SPECIFICATION

Please amend the paragraph [0078] beginning on page 41, as follows:

[0078] The prime candidate generation unit 142 judges whether a bit size "lenN" of the generated number "N" matches "~~lenq~~2×lenq". When determining that they match each other, the prime candidate generation unit 142 outputs the generated number "N" to the 1st primality testing unit 143, and stores, in the generated information storage area, the received random number "R1" as "R".

When determining that they do not match each other, the prime candidate generation unit 142 multiplies the random number "R1" received from the random number generation unit 141 by 2, makes the result "R1", and then generates the number "N = 2×R1×q+1" by conducting the above operation once again.

Please amend the paragraph [0150] beginning on page 66, as follows:

[0150] When determining that it is "information C" ("YES" in Step S505), the prime candidate generation unit 142 reads the prime "q" from the information storage area of the information control unit 140 (Step S510). The prime candidate generation unit 142 generates a number "N = 2×R1×q+1", using the read prime "q" and the random number "R1" received from the random number generation unit 141 (Step S515). The prime candidate generation unit 142 judges whether a bit size "lenN" of the generated number "N" matches "~~lenq~~2×lenq" (Step S520). When determining that they match each other ("YES" in Step S520), the prime candidate generation unit 142 outputs the generated number "N" to the 1st primality testing unit 143, and stores, in the generated information storage area, the received random number "R1" as "R" (Step S595).

Please amend the paragraph [0181] beginning on page 78, as follows:

[0181] Receiving the random number "R1" and control information from the random number generation unit 141A, the prime candidate generation unit 142A judges whether the received control information is "Information C".

When determining that it is "Information C", the prime candidate generation unit 142A reads the prime "q" from the information storage area of the information control

unit 140A. The prime candidate generation unit 142A generates a number "N = 2×R1×q+1", using the read prime "q" and the random number "R1" received from the random number generation unit 141A. The number "N" generated at this point becomes a prime candidate. The prime candidate generation unit 142A judges whether a bit size "lenN" of the generated number "N" matches "~~lenq~~2×lenq". When determining that they match each other, the prime candidate generation unit 142A outputs the generated number "N" to the 1st primality testing unit 143A, and stores, in the generated information storage area, the received random number "R1" as "R".

Please amend the paragraph [0205] beginning on page 86, as follows:

[0205] When determining that it is "Information C", the prime candidate generation unit 142B reads the prime "q" from the information storage area of the information control unit 140B. The prime candidate generation unit 142B generates a number "N = 2×R1×q+1" by using the read prime "q" and the random number "R1" received from the random number generation unit 141B. The number "N" generated at this point becomes a prime candidate. The prime candidate generation unit 142B judges whether a bit size "lenN" of the generated number "N" matches "~~lenq~~2×lenq". When determining that they match each other, the prime candidate generation unit 142B outputs the generated number "N" to the 1st primality testing unit 143B, and stores, in the generated information storage area, the received random number "R1" as "R".

Please amend the paragraph [0243] beginning on page 100, as follows:

[0243] Receiving the random number "R1" and control information from the random number generation unit 141C, the prime candidate generation unit 142C judges whether the received control information is "Information C".

When determining that it is "Information C", the prime candidate generation unit 142C reads the prime "q" from the information storage area of the information control unit 140C. The prime candidate generation unit 142C generates a number "N = 2×R1×q+1", using the read prime "q" and the random number "R1" received from the random number generation unit 141C. The prime candidate generation unit 142C judges whether a bit size "lenN" of the generated number "N" matches "~~lenq~~2×lenq". When

determining that they match each other, the prime candidate generation unit 142C outputs the generated number "N" to the 1st primality testing unit 143C, and stores, in the generated information storage area, the received random number "R1" as "R".

Please amend the paragraph [0256] beginning on page 105, as follows:

[0256] When determining that it is "information C" ("YES" in Step S705), the prime candidate generation unit 142C reads the prime "q" from the information storage area of the information control unit 140 (Step S710). The prime candidate generation unit 142C generates a number "N = 2×R1×q+1" by using the read prime "q" and the random number "R1" received from the random number generation unit 141C (Step S715). The prime candidate generation unit 142C judges whether a bit size "lenN" of the generated number "N" matches "~~lenq~~2×lenq" (Step S720). When determining that they match each other ("YES" in Step S720), the prime candidate generation unit 142C outputs the generated number "N" to the 1st primality testing unit 143C, and stores, in the generated information storage area, the received random number "R1" as "R" (Step S755).